基层事业单位网络安全技术防护及管理

摘　要：在网络信息化浪潮的不断推动下，网络规模迅速扩大，各个行业都主动融入其中，由此涌现出的互联网经济，不仅促进了企业的发展，而且给人们的生活带来了翻天覆地的变化。但随之而来的网络信息安全问题也日益突出。由于网络先天的脆弱性，导致黑客攻击、病毒泛滥等方面的问题层出不穷，给网络安全造成了威胁，甚至可能会造成一定的危害。因此，在享受网络带来的便利的同时，我们也应该对网络的安全问题保持高度警觉。本文阐述了基层事业单位所面临的网络安全问题以及相应的安全防护措施，涉及技术防范和安全管理，力图避免一些潜在的网络安全隐患发生，进一步提高基层事业单位计算机网络的安全性和可靠性。

关键词：基层事业单位；网络安全；安全防护
中图分类号：TP393　　文献标识码：A
文章编号：1671-0134（2019）06-110-03　　DOI：10.19483/j.cnki.11-4653/n.2019.06.033

文 / 张智伟

在信息技术飞速发展的今天，互联网络异军突起，以其易用、高效的便利性，轻松地融入了人们的工作和生活中。在享受科技带来乐趣的同时，也面临着来自网络层出不穷的各种威胁，信息安全不断受到挑战，特别是基础网络安全防护能力薄弱，导致安全危机。网络互联在基层事业单位已经完全普及，很多基层单位除了和上级单位连接的内部业务网络，还有根据自身业务接入互联网的独立局域网。基层事业单位的网络安全主要是解决自建网络的安全问题，网络规模不大，设备不多，但是种类与大型网络基本相同。随着互联网规模的膨胀，网络安全问题逐渐显现，而且越来越复杂，如果安全防护不到位，很容易受到病毒、木马等程序以及黑客的侵害，不仅会对本单位网络，甚至可能连同上级单位的网络一起会造成损害。因此，基层单位的网络必须要采用行之有效的技术手段和管理办法防范各种威胁网络安全的事件，尽量避免安全危害发生。

1. 网络安全概述

1.1 网络安全的定义

国际标准化组织 ISO 74982 文献中对安全的定义是：安全就是最大限度地减少数据和资源被攻击的可能性。《中华人民共和国计算机信息系统安全保护条例》第三条，规范了包括计算机网络系统在内的计算机信息系统安全的概念：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

1.2 网络安全的基本要素

从本质上讲，网络安全是指网络系统的硬件、软件和系统中的数据受到保护，不因偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统能连续可靠地正常地运行，网络服务不中断。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域，即网络安全的五个要素。

（1）保密性（Configentiality）：主要是指保证非授权的用户不能访问，信息不暴露给未授权的实体或进程。

（2）完整性（Integrity）：主要是指信息只有获得许可的用户才能修改实体或进程。

（3）可用性（Availability）：主要是指只有授权用户可以随时访问信息，有访问控制机制阻止非授权用户进入。

（4）可控性（Contrallability）：主要是指有授权机制、可对信息传播行为、内容和范围进行控制。

（5）不可否认性（Non-Repudiation）：主要是指出现的安全问题能提供监控、审计等手段，具备可追溯性。

网络的安全与开放是矛盾关系，系统不提供任何服务，不会产生安全威胁，一旦提供服务，在开放的网络环境下，各种安全问题必然随之而来。

2. 基层事业网络安全面临的问题

2.1 网络协议自身的缺陷

网络通信协议是互联网络传输的基础，协议设计之初，并没有考虑到现在网络的复杂情况，从而导致这些协议存在着不同的原生缺陷。TCP/IP 是 Internet 的基本协议，网络上针对它的缺陷有很多攻击方法。

物理层的侵害主要是对网络硬件和基础设施进行物理破坏。例如，施工将电力线路破坏引起单位断电，或者出口线路被挖断，均可导致无法访问互联网络。

ARP（地址解析协议）和 RARP（反地址解析协议）是 TCP/IP 数据链路层上的两个重要协议，ARP 欺骗和伪装是发生在这里的常见攻击手段。

网络层包括 ICMP、IP 和 IGMP 协议，它们常常引发大多数 ICMP 路由欺骗、Smuff 攻击和 IP 碎片攻击等著名

的网络攻击方式。

传输层是被攻击的重灾区，由于 TCP 连接占用资源大、释放慢和 UDP 无连接、不可靠等自身缺陷导致的攻击情况非常多，最常见的有会话劫持、中间人攻击、SYN FLOOD 攻击以及 TCP 序列号欺骗和攻击等。

在应用层上，应用协议众多，如 DNS、FTP、SMTP 等，主要攻击是 DNS 欺骗。此外，由于一些软件如数据库、自行开发的应用等软件在运行中出现漏洞，同样会引起黑客攻击。

2.2 恶意代码的危害

由于网络的开放、互联特性，网络上的用户可以自由来往于各个站点，各种信息系统互联互通，用户身份和位置难以识别，同时，由于网络协议和部分软件存在技术漏洞，这些都为恶意代码的传播和扩散提供了便利。常见的恶意蠕虫、病毒、缓冲溢出代码、后门木马等危害就是利用了 TCP/IP 协议的缺陷。越来越多的恶性攻击事件说明目前网络安全形势严峻，不法分子的技术手段也时常更新换代，网络的安全漏洞需要被网络管理员们时刻关注，网络安全的防范措施也要与时俱进能够应付不同的威胁，确保网络信息安全、可控。

2.3 人为因素

很多计算机用户网络安全意识差，加之使用不当，容易被敲诈、勒索等风险通过不安全网址或电子邮件植入木马后门，这些人为因素也会导致安全问题发生。

3. 网络安全防范措施

3.1 技术防范

3.1.1 物理安全

物理安全是保护计算机网络设备、设施及其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误或者各种针对网络或计算机的破坏行为。保证计算机信息系统各种设备的物理安全，是整个计算机信息系统安全的前提。

物理攻击分为偶然的和故意的，故意攻击是很明显的，网络的物理线缆或是设备、配套设施等被破坏，无法再提供网络服务；偶然事故和故意攻击本质不一样，但是结果是相同的，也会对网络或者某个设备造成破坏。偶然事故可以不归结于攻击。

物理环境安全主要是指对系统、设备所在的机房安全保护。保护措施和过程应按照国家有关设计标准实施，包括消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，应符合国家对不同等级机房的设计规范。

3.1.2 网络边界安全

网络安全主要包括网络运行和网络访问控制的安全。在内部网络与外部网络之间设置防火墙，实现对外部网络的隔离和访问控制，是保护内部网络安全的最主要措施，同时也是最优先、最经济的措施之一。

防火墙从实现原理上分为过滤防火墙、应用级网关防火墙、代理防火墙和规则检查防火墙，它们的部署位置完全取决于单位的访问要求和安全要求。客观地说，防火墙并不是解决网络安全问题的万能药方，而只是网络安全和策略中的一个组成部分，防火墙自身还有很多局限，例如，不能阻止利用协议缺陷的攻击、不能解决来自内部网络的攻击和安全问题等。所以，仅靠在互联网入口处设置防火墙是不能保护整个内部网络安全的，还应该配备 IPS（入侵防御系统）这样专门的安全设备来弥补防火墙的不足。IPS 位于防火墙和网络设备之间，可以配置深层次的防御安全策略，监视网络中的传输情况，通过对数据包的检测，及时调整或阻断一些不正常的传输，这是防火墙所无法做到的。IPS 作为必要的网络安全附加设备，已经为大多数单位网络安全架构的标配。

3.1.3 终端安全一体化安全防范

在当前的互联网环境下，一般基层事业单位已经建立了一个完整的网络平台，具备一定的网络规模，计算机终端数量较多。各种木马病毒、0day 漏洞，以及类似 APT 攻击等新型的攻击手段也越来越多，传统的防病毒技术以及管理手段已经无法满足现阶段网络安全的需要。目前，建立一体化终端安全和统一管理的网络威胁防护体系是一个单位整体防范网络安全威胁的首选。

国内绝大多数从事网络安全的公司都有面向企事业用户的网络安全管理系统，依托其各自的云安全系统，可提供整个网络终端安全状况评估，全面查杀、检测已知、未知病毒与恶意代码，通过云安全，实时更新安全补丁，调整威胁防护策略。通过对网络文件的安全审计和追踪，及时发现和定位未知威胁，可对终端漏洞修复、自动推送补丁，使网络终端的安全风险处于可管理、可控制状态。同时，还能将网络终端的整体安全状况和风险情况以数字化方式展现出来，帮助网络安全管理人员及时、准确、清晰地了解终端所处的风险状况，以便于快速解决问题。

3.2 管理措施

在网络安全领域的多年研究实践中，人们逐渐认识到管理在网络安全中的重要性，“三分技术，七分管理”的理念已经深入人心。网络安全同样遵循“木桶原理”，即一个木桶的容积取决于最短的那块木板，一个系统的安全强度等于最薄弱环节的安全强度。无论采用了多么先进的技术设备，还需要有以人为目标的管理手段来支持，只要安全管理上有漏洞，那么这个系统的安全一样没有保障。

3.2.1 定期检测网络状况

网络的状态是不断变化的，网络中的计算机所面临的威胁也随着网络环境在不断变化。网络管理员的岗位职责、日常工作要建章立制，包括定期检查联网计算机病毒代码更新情况，确保其处于最新版本，开启终端防护程序防关闭和防卸载功能，要经常通过一体化终端管理系统检查网络内终端安全状况，主动推送对网内终端的安全检测命令，使其在开机状态下自动修补安全漏洞。对于单位的内部计算机网络，更应严格控制输入输出，必要时应使用身份加密访问技术，通过对来访者身份的认证，确认是否有权限进行访问，这也是维护网络安全的一种有效方式。

此外，网络管理员要时常运用网络安全监测工具如

恶意软件分析包、网络流量分析工具、端口扫描工具和漏洞检测框架等网络安全性评估分析软件或硬件，检测系统的漏洞或潜在的威胁，发现隐患及时修补，以达到增强网络安全性的目的。

3.2.2 加强内部管理，强化安全意识

基层事业单位虽然人员相对固定和单一，但这并不意味着计算机在内部网络中使用就是安全的，网络安全威胁有的来自外部，有的则是来自单位内部。

基层单位没有专职的网络安全管理人员，防范力量较薄弱，首先要加强网络管理员的技术培训工作，有效补充新的网络安全管理知识，提高网络安全防范技术水平。

此外，单位内部每年应不定期开展网络安全自查工作，对于一些网络使用中存在的安全隐患进行总结，利用身边的案例开展多种形式的网络安全宣讲、教育活动。特别是要提高职工的安全意识，克制好奇心，不点击来路不明的邮件和链接，从而避免被植入木马、敲诈勒索以及诈骗等网络安全事件的发生。

培养职工使用移动存储先杀毒的良好习惯，鼓励个人使用正版软件，盗版软件本身就存在一定的安全威胁。同时，还需要完善一些监督机制，确保这些制度能够落到实处；否则，同样无法保障网络安全。

结语

网络安全防范是一个动态的过程，影响安全的因素都是动态变化的，防范也必然要通过一个动态的过程来实现。可靠的网络安全保障体系不仅具备对外部攻击进行有效防范的能力，还包括完善的内部安全管理制度，不应仅仅局限于对某种安全隐患的防范，还要具备应对各种网络安全隐患的整体解决能力，应当能够随着网络安全需求的变化而不断改进和完善。这就要求基层事业单位的网络管理员在日常工作中要加强对网络的全面监测，仔细观察和分析影响网络安全的相关因素，强化单位内部计算机的安全使用管理，最大程度地消除可能存在的安全隐患，确保基层事业单位的计算机网络安全平稳、可靠地有序运行。媒

参考文献

[1] 石淑华，池瑞楠 . 计算机网络安全技术（第 4 版）[M]. 人民邮电出版社，2016：5-6.

[2]（美）Douglas Jacobson 著，仰礼友，赵红宇，译 . 网络安全基础 - 网络攻防、协议与安全 [M]. 电子工业出版社，2016：262-270.

[3] 陈晓桦，武传坤 . 网络安全技术：网络空间健康发展的保障 [M]. 人民邮电出版社，2017：27-28.

（作者单位：新华社北京分社）

（上接第24页）

包括增强可理解性输入、友好的交互体系设计、UGC 与 PGC 关系的平衡以及利益分配与激励机制的设计等，鼓励和支持知识的输出行为，实现内容生产的闭环结构。媒

参考文献

[1] 杨鲁新 . 输出假设理论：历史与未来 [J]. 外语教学与研究：外国语文双月刊，2008（1）：45-50.

[2] 赵宏源 . 知识服务中交互的特殊性研究 [J]. 出版与印刷，2019（1）：6-11.

[3] 庄静 . 衍生作品的著作权问题 [J]. 特区经济， 2007（7）：215-217.

[4] 胡金梅 . 互动在语言输入和输出中的作用及其实证研究 [D]. 湖南：湖南科技大学，2006：1-82.

[5] 聂胜欣，俞树煜，袁梦霞 . 异步交互学习活动促进批判性思维发展实证研究 [J]. 现代远距离教育，2016（3）：60-67.

[6] 顾琦一 . 输出假说剖析 [J]. 外语学刊，2006（2）：77-83.

[7] 金涛 . 网络学习社区中促进知识深层建构的交互模式设计 [J]. 远程教育杂志，2015（3）：64-72.

[8] kennethan. 知识的特性 [OL] 简书 .https：//www.jianshu.com/p/1494feaff637，2018（4）：26.

[9] 巴志超 . 微信群内部的会话网络结构及关键节点测度研究 [J]. 图书情报工作，2017（20）：111-119.

[10] 张曼 . 输入、交互和输出与形式聚焦教学 [J]. 当代教育理论与实践，2011（2）：107-109.

[11] 王佳月 . 浅析思想与表达二分法原则 [J]. 商品与质量，2011（9）：16-17.

[12] 赵宏源 . 出版视域下的知识关联体系构建 [J]. 中国传媒科技，2019（1）：52-56.

（作者单位：上海世纪出版集团）